Thilo Weichert

Vorratsdatenspeicherung – unbeschränkt und überall!?

In der europäischen Öffentlichkeit wird seit dem Frühjahr 2001 über Vorratsdatenspeicherung diskutiert. Trotz klarstellender höchstrichterlicher Rechtsprechung ist die politische und juristische Debatte über den Zugriff von Sicherheitsbehörden auf die zunehmende Masse digitaler Datenbestände immer noch verhaftet im Konflikt um Meta-Daten aus der Telekommunikation. Digitale Menschenkontrolle ist aber inzwischen zu einem Phänomen geworden, das marktgetrieben insbesondere von privaten Unternehmen praktiziert wird, was sich der Staat zunutze macht bzw. machen kann. Es ist notwendig, eine umfassende Überwachungs-Gesamtrechnung durchzuführen und eine normative sowie praktische Einhegung vorzunehmen.

1. Kurze Geschichte

2001 wurden Forderungen einer europäischen Polizeiarbeitsgruppe bekannt, die Verbindungsdaten von Festnetz- und Mobil-Telekommunikation (TK) mindestens sieben Jahre lang zu archivieren und sicherheitsbehördlichen „Bedarfsträgern" zugänglich zu machen. Bis dahin war klar, dass derartige Verbindungsdaten frühestmöglich, also i. d. R. nach Ende der Verbindung bzw. spätestens nach erfolgter Abrechnung gelöscht bzw. anonymisiert werden. Zuvor schon war in Deutschland die Forderung nach Vorratsspeicherung von TK-Verbindungsdaten von Polizeibehörden erhoben und vom damaligen Bundesinnenminister Otto Schily bekräftigt worden. Seitdem tobt eine öffentliche Auseinandersetzung unter dem Begriff „Vorratsdatenspeicherung", bei der von Bürgerrechtsseite der Überwachungsstaat, von Sicherheitsbehörden die Kapitulation vor dem Verbrechen an die Wand gemalt wird.

Als Schily erkannte, dass er mit seinen Vorstellungen in Deutschland politisch nicht durchdringen würde, verlegte er sich darauf, über den Umweg der Europäischen Union (EU) die TK-Vorratsdatenspeicherung verpflichtend vorzusehen. Die damit verbundenen Normierungsbestrebungen auf europäischer wie auf nationaler Ebene sind bis heute nicht abgeschlossen. Der Europäische Gerichtshof (EuGH) hatte die verbind-

lichen Vorgaben auf EU-Ebene am 08.04.2014 für grundrechtswidrig erklärt[1] und dies mit Urteil vom 21.12.2016 bestätigt.[2]

Das aktuelle deutsche Gesetz, das am 18.12.2015 in Kraft trat[3], wird derzeit vor dem Bundesverfassungsgericht (BVerfG) angegriffen. Zuvor hatte das BVerfG mit Urteil vom 02.03.2010 eine frühere nationale Regelung wegen des Verstoßes gegen die Verfassung aufgehoben.[4]

Vorratsdatenspeicherung beschränkt sich nicht auf TK-Verbindungsdaten. Digitale Daten fallen bei immer mehr täglichen Verrichtungen an. Sie werden auch in anderen Zusammenhängen für Zwecke von Sicherheitsbehörden auf Vorrat gespeichert. So urteilte der EuGH am 26.07.2017 über eine Vorratsdatenspeicherung von Flugverkehrsdaten auf Grundlage eines geplanten Abkommens zwischen Kanada und der EU.[5]

2. Mehr als Telekommunikations-Verbindungsdaten

Künftig dürfte aus sicherheitsbehördlicher Sicht die Nutzung von digitalen Zahlungsdaten zunehmend relevant werden. Diese entstehen bspw. im Rahmen von Zahlungsvorgängen über das Internet sowie per Karte oder Smartphone am „Point of Sale" (POS), also an der Ladenkasse. Insofern gibt es noch keine umfassende Pflicht zur Vorratsdatenspeicherung; entsprechende Forderungen werden aber erhoben.[6] Die Pflicht zur ausnahmslosen Aufzeichnung von Online-Zahlungen wurde im Rahmen der 5. Geldwäsche-Richtlinie (5. AMLD)[7] erst nach Intervention des EU-Parlaments gestrichen. In der bis zum 10.01.2020 umzusetzenden EU-Richtlinie ist vorgesehen, dass anonyme E-Geld-Zahlungen am physischen POS statt bisher bis zu 250 € nur noch bis zu 150 € zulässig sind. Weiterhin besteht die Möglichkeit der Nutzung von anonymem Bargeld. Anonyme Zahlungen im Internet sind nach der 5. AMLD auf maximal 50 € pro Transaktion beschränkt. Angesichts des Umstands, dass die Nutzung von Bargeld immer weiter zurückgedrängt wird und diese teilweise selbst an Ladenkassen nicht mehr angenommen wird, drohen Verhältnisse, bei denen jede finanzielle Transaktion einer konkreten natürlichen Person zugeordnet werden kann. Zugleich werdender Zugriff auf die Finanztransaktionsdaten durch Sicherheitsbehörden erleichtert und technische Schnittstellen zu den Sicherheitsbehörden aufgebaut.

Konsum- und Finanztransaktionen sind hinsichtlich ihrer Aussagekraft über die Persönlichkeit der Betroffenen mit TK-Verkehrs- bzw. TK-Metadaten vergleichbar, auch wenn sie nicht, wie TK-Daten, durch das Telekommunikationsgeheimnis spezifisch verfassungsrechtlich geschützt sind (Art. 7 Grundrechte-Charta – GRCh; Art. 10 GG). Wohl aber kommt den Transaktionsdaten einfachgesetzlich über das Steuergeheimnis sowie über bankenrechtliche Vertraulichkeitszusicherungen ebenso ein verstärkter Schutz zu.

Eine dritte Dimension der Vorratsspeicherung eröffnet sich mit Mobilitätsdaten. Flugdaten, sogenannte *Passenger Name Records* (PNR), wie sie Grundlage für das Gutachten des EuGH zum Vertrag zwischen Kanada und der EU waren, sind nur die Spitze eines größeren „Datenbergs". Schon über Smartphones mit Lokalisierungsfunktion erfolgt heute, ohne gesetzlichen Zwang – auf einer in der Praxis wenig freiwilligen Basis und völlig intransparent – für die Betroffenen eine räumlich-zeitliche Zuordnung

der meisten Mobilfunkgeräte. Mit der zunehmenden Online-Anbindung von Kfz entstehen nicht nur für Netz-, Plattform-, Dienste- und App-Anbieter, sondern auch über die Kfz-Hersteller Mobilitätsdaten, die konkreten Personen zuzuordnen sind. Diese Mobilitätsdaten genießen keinen speziellen verfassungsrechtlichen Schutz. Das Netz schützender einfachgesetzlicher Regelungen ist leider stark durchlässig.

Das Überwachungsnetz zur Mobilität wird, getragen von der technischen Weiterentwicklung, zunehmend enger: Die klassische Jedermann-Kontrolle erfolgte bisher über die Videoüberwachung. Bei deren Einsatz im öffentlichen Raum besteht eine nahezu unbegrenzte Streubreite. Lange Zeit war eine Individualisierung der Bilder schwierig und fehleranfällig. Dies ändert sich mit Fortschritten bei der Bildmuster- und Gesichtserkennung. Liegen digitalisierte Gesichtsbilder vor, auf die z. B. Sicherheitsbehörden schon heute über Personalausweis- und Passregister Zugriff haben,[8] können Personen einem Ort, zu dem sie sich zu einem bestimmten Zeitpunkt aufhielten, präzise zugeordnet werden. Diese Praxis wird in Berlin am Bahnhof Südkreuz erprobt. Eine technisch weniger anspruchsvolle, aber dafür schon vollautomatisierte Form eines solchen Einsatzes von Mustererkennung per Video für Sicherheitszwecke ist das Kfz-Kennzeichen-Scanning, zu dem das BVerfG am 18.12.2018 seine verfassungsrechtlichen Anforderungen konkretisierte.[9]

3. Verfassungsrechtlicher Rahmen

Das Spezifische der TK-Vorratsdatenspeicherung war und ist, dass zu einem für einen ursprünglich konkreten Zweck verarbeitete Daten ausschließlich für sicherheitsbehördliche Zwecke weiter aufbewahrt werden, ohne dass absehbar ist, dass die erfassten Daten zu aus Sicherheitssicht unauffälligen Personen von konkretem Nutzen sein werden.

Verfassungsrechtliche Ansatzpunkte für die Bewertung der Vorratsdatenverarbeitung sind das allgemeine Persönlichkeitsrecht (Art. 2 Abs.1 i. V. m. Art. 1 Abs. 1 GG) bzw. das Grundrecht auf Datenschutz (Art. 8 GRCh) in Verbindung mit weiteren Freiheitsrechten, etwa dem Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh). Die Schutzwirkung dieser Grundrechte beschränkt sich nicht auf die erstmalige Erhebung von Daten, sondern erstreckt sich auch auf deren weitere Nutzung. Die hoheitliche Eingriffsqualität besteht nicht nur, wenn die Daten direkt von staatlichen Einrichtungen erfasst werden, sondern ebenso, wenn diese die Daten bei Privaten beschaffen, wo sie zuvor erhoben wurden.[10]

Staatliche Eingriffe müssen durch ein Gesetz präzise und bereichsspezifisch erlaubt sein, das legitimen Gemeinwohlinteressen dient und dem Grundsatz der Verhältnismäßigkeit genügt, das also zur Erreichung der Zwecke geeignet, erforderlich und angemessen ist (Art. 52 Abs. 1 GRCh). Dabei ist es nötig, dass die betroffenen Daten sowie die Formen der Datenverarbeitung präzise, d. h. hinreichend bestimmt beschrieben werden. Dies gilt insbesondere, wenn auf der Datenbasis automatisierte Analysen durchgeführt werden. Dann muss gewährleistet sein, dass die angewendeten Modelle und Kriterien spezifisch und zuverlässig sind und eine Identifizierung nur erfolgt, wenn ein begründeter Verdacht vorliegt und dabei keine Diskriminierung erfolgt.[11]

In der Rechtsprechung des BVerfG wurde aus den Freiheitsrechten schon früh ein striktes „*Verbot einer Speicherung von Daten auf Vorrat*“ abgeleitet. Verboten ist die Verarbeitung von Daten zu unbestimmten und noch nicht bestimmbaren Zwecken.[12]

Das BVerfG weist seit dem Volkszählungsurteil darauf hin, dass personenbezogene Datenspeicherung eine abschreckende Wirkung für die Wahrnehmung von Freiheitsrechten haben kann und benennt ausdrücklich die politischen Rechte auf „*Teilnahme an einer Versammlung oder einer Bürgerinitiative*“. Der Mensch muss wissen können, „*wer was wann bei welcher Gelegenheit über ihn weiß.*“ Informationelle Selbstbestimmung ist „*eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens*“.[13] Der Bundesgerichtshof nimmt ein Recht auf Anonymität auch in Bezug auf die Wahrnehmung der Informations- und Meinungsfreiheit an.[14]

Zur Freiheitlichkeit des Gemeinwesens gehört es auch, „*dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein*“.[15] Datenverarbeitung darf deshalb nicht „einfach drauflos“, zu beliebiger Zeit und an beliebigem Ort „ins Blaue hinein“ und „für alle Fälle“ erfolgen. Ein „bloßer Betriebsverdacht“ genügt nicht.[16] Das BVerfG hat die gesellschaftliche Relevanz des Rechts auf Anonymität mit seiner Feststellung akzentuiert, dass es „*zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland*“ gehört, in der persönlichen Freiheitswahrnehmung nicht total erfasst und registriert zu werden (dazu ausführlich unten 6).[17]

4. Abwägung mit legitimen Zwecken

Als „legitime Zwecke“ für eine sicherheitsbehördliche Datenverarbeitung sind die Effektivierung der Strafverfolgung, die Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste anerkannt. Der Staat „*hat einen wirksamen Schutz der Grundrechte und Rechtsgüter der Bürgerinnen und Bürger zu sichern.*“ Die Sicherheit des Staates als verfasste Friedens- und Ordnungsmacht und die von ihm – unter Achtung von Würde und Eigenwert des Einzelnen – zu gewährleistende Sicherheit der Bevölkerung (sind) Verfassungswerte, die mit anderen hochwertigen Verfassungsgütern im gleichen Rang stehen.[18]

Bei einer verfassungsrechtlichen Bewertung geht es darum, die Geeignetheit, die Erforderlichkeit und die Angemessenheit der konkreten Datenverarbeitung für die Sicherheitszwecke zu begründen. Bei der rechtlichen Prüfung läuft es dabei zumeist darauf hinaus, die Angemessenheit, also die Verhältnismäßigkeit „im engeren Sinne“ festzustellen.

Es kommt dabei darauf an, woran die hoheitliche Datenverarbeitung anknüpft: Ist Anknüpfungspunkt ein zurechenbares, vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation; oder geht es um Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist? Schwer ist ein Eingriff, wenn Betroffene, „*ohne selbst Anlass dazu gegeben zu haben*“, dem Risiko von Ermittlungen

ausgesetzt werden.[19] Bei einem gefährlichen oder risikobehafteten Tun bzw. zur Beherrschung besonderer Gefahrenquellen sind dagegen anlasslose Kontrollen nicht generell ausgeschlossen. Eine spezifische Eigenschaft der Vorratsdatenverarbeitung ist deren Streubreite.[20] Es darf dabei keine flächendeckende Totalerfassung, keine „Rundumüberwachung" erfolgen.[21]

Die Eingriffsintensität wird zudem durch die Missbrauchsmöglichkeiten der Datenverarbeitung bestimmt, wobei als Agierende sowohl staatliche Einrichtungen, die privaten Verarbeiter wie auch Dritte in Betracht zu ziehen sind. Bei einer sensitiven Datenverarbeitung ist ein besonders hohes Sicherheitsniveau gefordert. Werden die Daten automatisiert analysiert, so sind Sicherungsmaßnahmen erforderlich, damit auf dieser Basis keine fehlerhaften oder diskriminierenden Entscheidungen getroffen werden (vgl. Art. 22 DSGVO).[22]

5. Kriterien

Für die Verhältnismäßigkeit ist die Speicherdauer von Relevanz. Generell gilt, dass diese hinsichtlich der jeweiligen Zweckerreichung so kurz wie möglich sein muss (vgl. Art. 5 Abs. 1 lit. e DSGVO). Dass das BVerfG im Jahr 2010 bezüglich der TK-Vorratsdatenspeicherung grundsätzlich eine sechsmonatige Speicherdauer noch als angemessen bewertet hat, war wohl dem Umstand zuzuschreiben, dass bei einer anderen Bewertung eine Vorlage des Verfahrens vor dem EuGH notwendig gewesen wäre, was vermieden werden sollte. Die Speicherdauer ist auf „das absolut Notwendige" zu beschränken.[23]

Hinsichtlich der Speicherdauer wie der Erhebungs- sowie der Nutzungsvoraussetzungen muss nach der Art der Daten differenziert werden. So kann die Speicherung von reinen Pseudonymen ein geringerer Eingriff als die Speicherung identifizierter Datensätze sein. Angaben aus der Sphäre der Öffentlichkeit sind weniger schutzbedürftig als solche aus dem Sozialbereich oder aus der Intimsphäre. Ein Aspekt bei der Abwägung ist, inwieweit die Datenspeicherung zur Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile geeignet ist.[24] Einer zweckspezifischen Legitimation bedarf es bei sensitiven Daten (vgl. Art. 9 Abs. 1 DSGVO). Absolut tabu ist der „Kernbereich privater Lebensgestaltung".[25] Das Gleiche gilt in Bezug auf Vorratsdatenverarbeitungen für Berufsgeheimnisse.[26]

Um Eingriffsmaßnahmen auf das „absolut Notwendige" zu beschränken, sind als Erhebungsvoraussetzungen restriktive differenzierte Festlegungen in Bezug auf Anlass, Ort und Zeit nötig. Grundlage der Festlegungen müssen objektive, überprüfbare Anhaltspunkte und Sachverhalte sein.

Als prozedurale Kriterien sind „*eine für die Öffentlichkeit transparente Kontrolle unter Einbeziehung des unabhängigen Datenschutzbeauftragten sowie ein ausgeglichenes Sanktionensystem, das auch Verstößen gegen die Datensicherheit ein angemessenes Gewicht beimisst*", anerkannt.[27] Als Transparenzaspekte kommen in Betracht: die Offenheit der Erhebung und der Nutzung der Daten sowie die nachträgliche Benachrichtigung gegen über Betroffenen. Hierüber kann auch ein effektiver Rechtsschutz gewährleistet werden. Zusätzlich möglich sind spezielle Anordnungsvorbehalte, etwa durch einen

unabhängigen Richter. Der Transparenz dienen weiterhin Begründungs- und Dokumentationspflichten. Zur Gewährleistung der Einhaltung der Nutzungsregelungen ist eine effektive unabhängige Datenschutzkontrolle nötig, über die auch gewährleistet wird, dass Verstöße erkannt und sanktioniert werden.

Notwendig ist nicht nur ein gesetzlich klar definierter enger Rahmen für die Erfassung und Speicherung, sondern auch für die Verwendung der auf Vorrat gespeicherten Daten.

In Bezug auf die TK-Vorratsdatenspeicherung verlangt das BVerfG bzgl. der Strafverfolgung „*zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat*". Dabei kann auf einen Katalog zurückgegriffen oder an den jeweils angedrohten Strafrahmen angeknüpft werden. Ergänzend muss für den konkreten Einzelfall die Verfolgung einer schweren Straftat vorliegen. Auch gemäß dem EuGH ist „*allein die Bekämpfung der schweren Kriminalität*" zur Rechtfertigung des Einsatzes dieser Maßnahme in der Lage.[28]

Bei der Gefahrenwehr kann nicht an einen Katalog von Straftaten angeknüpft werden, die es zu verhindern gilt. Vielmehr müssen das maßgebliche Ziel des konkret verfolgten Rechtsgüterschutzes und die Intensität der Gefährdung dieser Rechtsgüter zur Grundlage genommen werden. Das BVerfG verwendet bei massiven Eingriffen als Rechtsfertigungskategorie die „*Abwehr von Gefahren für Leib und Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr*". Die konkrete Gefahr wird näher beschrieben durch „*den Einzelfall, die zeitliche Nähe des Umschlagens einer Gefahr in einen Schaden und den Bezug auf individuelle Personen als Verursacher*". Zur Abwehr einer „drohenden Gefahr" sind Jedermannkontrollen und Vorratsdatenspeicherungen in jedem Fall unverhältnismäßig.[29]

Für eine Nutzung von Vorratsdaten durch Nachrichtendienste sind wegen der Zuordnung zum präventiven Bereich die gleichen Anforderungen wie bei der Gefahrenabwehr zu stellen. Da diese Dienste aber oft weit im Vorfeld von Gefahren agieren, scheidet insofern eine Nutzung von Vorratsdaten regelmäßig aus.[30]

6. Überwachungs-Gesamtrechnung

Die übermäßigen Überwachungsregelungen zum Polizeiaufgabengesetz Bayerns (PAG)[31] brachten einen Passus des Urteils des BVerfG zur Vorratsdatenspeicherung aus dem Jahr 2010 in die Diskussion zurück: Dass die Wahrnehmung der Freiheitsrechte nicht total erfasst und registriert werde, gehöre „*zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland*".[32]

Zur verfassungsrechtlichen Identität der Bundesrepublik gehört es, dass eine „*möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten*" unzulässig ist. Die vorsorglich anlasslose Speicherung muss die Ausnahme bleiben: „*Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen.*" Die Datenspeicherung darf zudem nicht durch den Staat direkt, sondern allenfalls durch private Stellen erfolgen und nicht die (Kommunikations-) Inhalte erfassen.

Der Gesetzgeber ist, so das BVerfG, gezwungen, „*bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen*“ Zurückhaltung zu üben. Durch vorsorgliche Datenspeicherungen wie z. B. der TK-Verkehrsdaten werde „*der Spielraum für weitere anlasslose Datensammlungen*“ geringer.[33]

7. Multiple Verarbeitungen für multiple Zwecke

Das BVerfG hatte bei seinen Ausführungen die Vorratsspeicherung von TK-Verkehrsdaten im Blick, die mit der Wahrung und Herstellung der inneren Sicherheit begründet war. Dieser anlassbezogen richtige Ansatz muss indes bei der Erstellung einer Überwachungs-Gesamtrechnung erweitert werden: Nicht nur das Datenvolumen und die Datenqualität explodieren derzeit in der Praxis, sondern auch deren Verwendbarkeit. Die Zeiten, in denen Daten nur für einen Zweck erhoben wurden, sind schon längere Zeit vorbei. Die europäische Datenschutz-Grundverordnung hat hieraus den konsequenten Schluss gezogen, dass die – im Gemeinwohl erfolgende – Zweitverwertung von Daten für Zwecke der Forschung (sowie der Statistik und des Archivwesens) privilegiert wird (Art. 5 Abs. 1 lit. b DSGVO). Mit dieser Privilegierung einhergehen muss eine Abschottung von weiteren Nutzungen und Begehrlichkeiten. Eine ähnliche mit einer strengen Nutzungseinschränkung verbundene Privilegierung kennen wir im deutschen Datenschutzrecht mit der Verwendung von Daten für Zwecke der Datensicherheit und Datenschutzkontrolle (so der bis zum 25.05.2018 anwendbare § 31 BDSG-alt).

TK-Verkehrsdaten sind ein gutes Beispiel für die Ausweitung der Verwendbarkeit. Nicht zuletzt wegen ihrer multiplen Zweckgeeignetheit werden diese auch nicht mehr „Verkehrsdaten“ bzw. „Nutzungsdaten“, sondern präziser „Meta-Daten“ genannt. Die weitere Nutzung für andere Zwecke erfolgt normativ durch eine Abwägung zwischen den legitimen Nutzungsinteressen und den Schutzinteressen der Betroffenen (vgl. Art. 6 Abs. 1 S. 1 lit. f DSGVO). Von der Datenschutzpraxis wurde schon weitgehend der Zweck der „Verbesserung“ des Serviceangebots durch den Verantwortlichen anerkannt. Normativ hatte dieser Zweck eine Grundlage in § 15 Abs. 3 S. 1 TMG, wonach Nutzungsdaten „*für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung*“ verwendet werden dürfen. Die Nutzung dieser Formel hat sich inzwischen praktisch dahin gewendet, dass Verantwortliche Meta-Daten zur verbesserten Manipulation der Betroffenen nutzen.

Während diesen Nutzungszwecken von Rechtswegen mit Widerspruchsmöglichkeiten noch Einhalt geboten werden kann und es bei den Zwecken auf den individuellen Datensatz regelmäßig nicht ankommt, ist die Nutzung für Zwecke der Datensicherheit vom konkreten Datensatz abhängig. Der bürgerrechtliche Widerstand gegen diesen Verwendungszweck war bei TK-Meta-Daten lang anhaltend[34] und wurde – zu Recht – durch höchstrichterliche Rechtsprechung gebrochen, als der EuGH am 19.10.2016 feststellte, dass die Verarbeitung von Meta-Daten sich nicht auf die „*konkrete Inanspruchnahme des Dienstes durch den fraglichen Nutzer*“ beschränken kann, sondern die generel-

le Gewährleistung „*der Funktionsfähigkeit der Dienste*“ mit einschließt, wozu die informationstechnische Sicherheit gehört.[35]

Inzwischen werden durch private Betreiber von Applikationen und Plattformen massenhaft personenbezogene Daten erfasst, die nicht nur für die Erbringung der immer komplexer gestalteten Dienste erforderlich sind, sondern die weit darüber hinausgehen. Auch was die Dauer der Datenspeicherung angeht, gibt es bei vielen Betreibern in der Praxis keine Grenzen. Das Geschäftsmodell von Facebook und Google besteht z. B. darin, Alltagsverrichtungen digital zu erfassen und daraus Querschnitts- und Leitzeitprofile zu erstellen, die zur Grundlage für (Online-)Werbung genutzt werden. Dabei erfolgt derzeit schon eine zeitlich unbegrenzte, anwendungsübergreifende Totalüberwachung. Der von diesen Betreibern verfolgte Zweck liegt dabei nicht nur in der Werbung; der Zweck liegt – übergreifender –in der Totalüberwachung selbst. Insofern kann nicht mehr von Vorratsspeicherung, es muss vielmehr von dauernder Verwendungsspeicherung gesprochen werden. Diese Daten sind potenziell und gesetzlich für Sicherheitsbehörden zugänglich, nicht nur in den USA, sondern auch in Deutschland. Über die StPO, über das Polizeirecht oder über sonstiges Sicherheitsrecht kann zwingend – zumindest bei konkreten Anlässen – ein staatlicher Zugriff erfolgen. Dies geht so weit, dass Sicherheitsbehörden schon zwingend Zugriff direkt bei den Betroffenen auf Ton- und Bilddaten nehmen wollen, ohne dass diese Störer sind.[36]

Wir befinden uns derzeit mitten in einer Digitalisierungsphase, bei der das technische Potenzial noch nicht ansatzweise ausgeschöpft ist. Potenziale bestehen z. B. in den Kameras und Mikrophonen von stationären und mobilen Geräten, vom Fernsehgerät bis zum Smartphone, die – einmal initialisiert – optischen und akustischen Einblick in Schlaf- und Wohnzimmer sowie in sämtliche tägliche Verrichtungen erlauben. Potenziale bestehen bei Gesundheits- und Wellness-Apps, die Einblick in das körperliche und seelische Befinden geben. Gewaltige Potenziale liegen noch weitgehend im biotechnischen Bereich brach, der derzeit z. B. über reine Lifestyle-Angebote dabei ist, auch in Europa Fuß zu fassen.[37] Der digitale Griff auf individuelle Gefühle und Gedanken wie auf genetische Dispositionen ist schon im Gange.

8. Überwachungs-Gesamtrechnung weiter gedacht

Die Ausführungen des BVerfG zur Überwachungs-Gesamtrechnung wurden zwar im Kontext der europäischen Integration gemacht, gelten aber selbstverständlich ebenso für rein nationale Normierungen und binden nicht nur den Bundes-, sondern auch die Landesgesetzgeber. Sie haben nicht nur die Telekommunikation, sondern generell die Digitalisierung des Alltags im Blick. Erfasst wird nicht nur die hoheitliche Datenerfassung, sondern auch die durch private Unternehmen. Ähnlich wie bei der Verhältnismäßigkeitsprüfung generell kann die Grenze des noch Erlaubten nicht präzise bestimmt werden. Wohl aber kann deren Überschreitung anlassbezogen verbindlich festgestellt werden. Dabei ist der gesamte Instrumentenkasten einzubeziehen, den die Rechtsprechung zur Einhegung der Überwachung entwickelt hat (s. 5.). Diese Instrumente sind weiter zu entwickeln.

Der Gesetzgeber ist verpflichtet, dauernd nicht nur die Gesetzgebung, sondern auch die gelebte Praxis der Überwachung zu beobachten.[38] Er muss intervenieren, wenn durch private Unternehmen ein Überwachungspotenzial etabliert wird, mit dem unsere Verfassungswerte gefährdet werden.[39] Die Erstellung der Gesamtrechnung ist also kein einmaliger Vorgang, sondern muss ein dauernder Prozess sein. Bei diesem Prozess können Erfahrungen aus anderen Teilen der Welt erkenntnisfördernd sein, etwa der Blick in die USA, nach China oder nach Russland.

Natürlich besteht, gerade mit Blick auf Überwachungspraktiken in anderen Staaten, die Gefahr, dass die Formel zur „Überwachungs-Gesamtrechnung" für Rechtfertigungsrhetorik genutzt wird.[40] Dass dies nicht erfolgreich ist, setzt eine Operationalisierung voraus. Diese besteht in einer Präzisierung der „doppelten Verhältnismäßigkeitsprüfung", also neben der Prüfung der konkreten Maßnahme die Erstellung einer Gesamtbewertung.

Diese Gesamtbewertung ist ohne empirische Feststellungen unmöglich. Da die Digitalisierung des Alltags der Menschen vorrangig im privaten Sektor stattfindet, muss hier ein Schwerpunkt gesetzt werden. Die Evaluation des staatlichen Zugriffs auf die privat gesammelten Daten kann nur der zweite Schritt sein. Angesichts der Rechtspositionen der Datensammler in der Wirtschaft, die sich auf ihre Betriebs- und Geschäftsgeheimnisse berufen, bedarf es der gesetzlichen Regulierung der staatlichen Einblickmöglichkeiten in die privatwirtschaftliche Verarbeitung mit Daten der Bürgerinnen und Bürger.

Bei der Herstellung dieser Transparenz, also bei der Überwachung der Überwachung, kommt es auf die Art der Daten, deren Speicherung und deren Sensitivität für die Freiheitswahrnehmung ebenso an wie auf deren weitere Verarbeitung und Auswertung. Die Datenanalyse darf nicht länger, wie bisher, dem unternehmerischen Arkanbereich vorbehalten bleiben. Dies gilt nicht nur (worüber derzeit eine gewisse Debatte stattfindet) für den Einsatz künstlicher Intelligenz, sondern für jede Form der komplexen Auswertung von Bürgerdaten. Bisher ist den technischen Schnittstellen zwischen den verschiedenen Datenbeständen, insbesondere denen zwischen dem privaten Bereich und staatlichen Behörden, wenig Aufmerksamkeit gewidmet worden. Wegen der sich dadurch ergebenden zusätzlichen Überwachungsrisiken muss sich dies ändern.

9. Abschließende Bemerkung

Die Diskussion um die Vorratsspeicherung war und ist wichtig. Sie ist geeignet, äußere Rahmenbedingungen für die Digitalisierung unserer Lebenswelt zu definieren. Das BVerfG und der EuGH haben hierzu Bewertungskriterien benannt. In Zeiten von *Big Data* wird die anlasslose Datenerfassung und -speicherung zunehmen. Diese dient immer weniger ausschließlich hoheitlichen Sicherheitszwecken und muss deshalb auch nicht gesetzlich angeordnet werden. Sie erfolgt – angesichts der beliebig großen Zahl möglicher Zwecke – gezielt und oft zeitlich unbegrenzt. Dies macht es nötig, bei der Diskussion über die Vorratsdatenspeicherung nicht stehen zu bleiben. Ein zentraler Ansatzpunkt für die Weiterentwicklung der Auseinandersetzung sollte sein, die digi-

talen Spuren, die im privaten Bereich derzeit hinterlassen werden, zurückzudrängen und zugleich den möglichen staatlichen Zugriff auf diese Daten rechtlich zu beschränken. Diese Weiterentwicklung des Rechts ist auf allen Ebenen nötig: auf Verfassungsebene, etwa durch digitale Grundrechte[41], im Völkerrecht, etwa zur Verhinderung der globalen Bespitzelung, wie sie seit 2013 insbesondere durch Edward Snowden bekannt gemacht wurde,[42] im Rahmen der EU durch Präzisierung der Grundsätze der DSGVO, wie auch national. Die Regulierung durch Bundesländer und auf Bundesebene eignet sich nicht zuletzt als Erprobungsfeld für Europa zur Sicherstellung des Grundanspruchs auf unbeobachtete Freiheitsbetätigung; sie bleibt aber vor allem die wichtigste Regulierungsebene zur Abwehr übermäßiger Überwachungsbegehren der nationalen und regionalen Sicherheitsbehörden.

DR. THILO WEICHERT Jahrgang 1955, studierte Rechts- und Politikwissenschaften und promovierte mit einer Arbeit zum Datenschutz im strafrechtlichen Ermittlungsverfahren. Er gehörte von 1984 bis 1986 dem Landtag von Baden-Württemberg an, danach war er als Rechtsanwalt und Berater und ab 1992 als Referent beim niedersächsischen Datenschutzbeauftragten tätig. 1998 wechselte er nach Schleswig-Holstein, wo er von 2004 bis 2015 Datenschutzbeauftragter des Landes war. Er ist Mitglied des Netzwerks Datenschutzexpertise (www.netzwerk-datenschutzexpertise.de) und Vorstandsmitglied der Deutschen Vereinigung für Datenschutz (DVD).

Anmerkungen:

1 EuGH 08.04.2014 – C-293/12, C-594/12 (Vorratsdaten I).
2 EuGH 21.12.2016 – C-203/15, C-698/15 (Vorratsdaten II).
3 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten v. 10.12.2015, BGBl. I S. 2218.
4 BVerfG 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 (Vorratsdaten).
5 EuGH 26.07.2017 – Gutachten 1/15 (PNR).
6 Weichert, Das Recht auf Anonymität finanzieller Transaktionen, 27.12.2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_5gwrl271216.pdf, S. 12 ff.
7 5. Anti-Money-Laundering-Directive, Richtlinie (EU) 2018/843 v. 30.05.2018, ABl. L 156/43.
8 S. Gesetz zur Förderung des elektronischen Identitätsnachweises v. 07.07.2017, BGBl. I S. 2310, z. B. § 15 Abs. 1 S. 2 PAuswG.
9 BVerfG 18.12.2018 – 1 BvR 142/15 (Kfz-Kennzeichen II) und 1 BvR 2795/09, 1 BvR 3187/10.
10 BVerfG 02.03.2010 (Anm. 4) Rn. 190, 193-196.
11 EuGH 26.07.2017 (Anm. 5) Rn. 168-174.
12 BVerfG 15.12.1983 – 1 BvR 209/83 u. a. (Volkszählung) Rn. 101, NJW 1984, 422; BVerfG 02.03.2010

(Anm. 4) Rn. 205f.
13 BVerfG 15.12.1983 (Anm. 12) Rn. 94; zur gesellschaftlichen Bedeutung der Meinungsfreiheit EuGH 21.12.2016 – C-203/15, C-698/15 Rn. 93.
14 BGH 23.06.2009 – VI ZR 196/08 Rn. 38; indirekt auch EuGH 21.12.2016 (Anm. 2) Rn. 101.
15 BVerfG 18.12.2018 (Anm. 9) Rn. 51.
16 BVerfG 02.03.2010 (Anm. 4) Rn. 261; BVerfG 18.12.2018 (Anm. 9) Rn. 92; BVerfG 24.05.1977 – 2 BvR 988/75 (Drogenberatungsstelle) Rn. 82.
17 BVerfG 02.03.2010 (Anm. 4) Rn. 218.
18 BVerfG 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 (BKA-Gesetz) Rn. 100.
19 BVerfG 02.03.2010 (Anm. 4) Rn. 212.
20 BVerfG 18.12.2018 (Anm. 9) Rn. 94; BVerfG 02.03.2010 (Anm. 4) Rn. 213.
21 BVerfG 02.03.2010 (Anm. 4) Rn. 218; BVerfG 12.04.2005 – 2 BvR 581/01 (GPS) Rn. 60; BVerfG 18.12.2018 (Anm. 9) Rn. 115.
22 EuGH 26.07.2017 (Anm. 5) Rn. 173 f.
23 EuGH 26.07.2017 (Anm. 5) Rn. 140; EuGH 21.12.2016 (Anm. 2) Rn. 96; EuGH 08.04.2014 (Anm. 1) Rn. 52.
24 BVerfG 02.03.2010 (Anm. 4) Rn. 211; ständige Rechtsprechung seit BVerfG 16.07.1969 – 1 BvL 19, 63; BVerfGE 27, 1 (Mikrozensus); NJW 1969, 1707.
25 BVerfG 20.04.2016 (Anm. 18) Rn. 120.
26 BVerfG 20.04.2016 (Anm. 18) Rn. 131, 133; EuGH 21.12.2016 (Anm. 2) Rn. 105; EuGH 08.04.2014 (Anm. 1) Rn. 58.
27 BVerfG 02.03.2010 (Anm. 4) Rn. 225; ähnlich BVerfG 20.04.2016 (Anm. 18) Rn. 135; BVerfG 18.12.2018 (Anm. 9) Rn. 101; EuGH 21.12.2016 (Anm. 2) Rn. 120; EuGH 26.07.2017 (Anm. 5) Rn. 192, 202.
28 BVerfG 02.03.2010 (Anm. 4) Rn. 228 f.; EuGH 21.12.2016 (Anm. 2) Rn. 102; EuGH 08.04.2014 (Anm. 1) Rn. 60.
29 BVerfG 02.03.2010 (Anm. 4) Rn. 231; EuGH 26.07.2017 (Anm. 5) Rn. 179 f.; vgl. BVerfG 18.12.2018 (Anm. 9) Rn. 105.
30 BVerfG 02.03.2010 (Anm. 4) Rn. 233 f.
31 G. v. 18.05.2018, BayGVBl. S. 301, 434.
32 BVerfG 02.03.2010 (Anm. 4) Rn. 218.
33 BVerfG 02.03.2010 (Anm. 4) Rn. 218.
34 Dazu Weichert in BvD-News 02/2015, 19 ff.
35 EuGH 19.10.2016 – C-582/14 Rn. 50-64.
36 So z. B. § 32a NPOG-E, Nds. LT-Drs. 18/850 v. 08.05.2018.
37 Weichert, AncestryDNA ist in Deutschland, www.netzwerk-datenschutzexpertise.de v. 17.12.2018.
38 BVerfG 12.04.2005 – 2 BvR 581/01 Rn. 51, 64.
39 BVerfG 23.10.2006 – 1 BvR 2017/02, Rn. 29, 31-36; BVerfG 17.07.2013 – 1 BvR 3167/08, Rn. 18-20.
40 Roßnagel in NJW 2010, 1242.
41 Vgl. Charta der Digitalen Grundrechte der Europäischen Union, https://digitalcharta.eu/.
42 Weichert in DuD 2014, 402.